Future Ready Schools - NJ

Indicators of Future Readiness

Indicator	**Data Security and Privacy**
Theme	**Technology Support and Services**
Gear	**Data and Privacy**
Priority Level	**P1**
Organizational Level	**District**

Description of the Indicator

Districts need to take reasonable steps to ensure the security of data systems in addition to the integrity and privacy of collected data. Policies and procedures should be developed to ensure the data systems they host are secure and data systems that they interact with have sufficient breach notification and strong privacy policies. Policies should also provide role-specific guidance to staff to safeguard data and ensure best practices are followed when accessing, collecting, storing and/or using data.

Why is this indicator important to creating a Future Ready School?

As Districts collect more information about our students and staff it is vital that the data be kept private and secure. This is not only a regulatory requirement, but part of the essential trust between a District and their students, parents and staff.

Indicator Rubric

Insufficient Evidence of Implementation **(0 Points)**	● The district has not started the process of identifying/classifying data and assigning data stewards to systems ● There are no policies or the district is in the process of drafting policies and procedures ● There is no existing process for incident responses ● Districts have not started dialogue with Third-Party vendors regarding policies and procedures to protect students and faculty data
Foundational Stage of Implementation **(3 Points)**	● The district started the process of identifying and classifying data in their systems and is in the process of assigning roles and data stewards for all systems ● Policies and procedures are being created or revised ● The district has initiated the conversation with Third-Party vendors to address the need to align data security/privacy policies and procedures
Achieving Success in Implementation **(6 Points)**	● District data has been identified, classified, and assigned to the right users and has been placed under the guidance of designated data stewards ● Policies and procedures designed to protect student and faculty data have been Board approved and communicated to students, faculty, and parents ● The district is developing policies and procedures with Third-Party vendors that follow best practices and industry standards to protect student data and privacy ● Incident Response Plans are in the development stage
Exemplary Success in Implementation **(9 Points)**	● The district has taken the necessary steps to protect the integrity and privacy of collected data in all systems ● Data has been identified, classified, and assigned to the right users and has been placed under the guidance of designated data stewards ● Policies and procedures designed to protect student and faculty data have been Board approved and communicated to students, faculty, and

	parents ● The district has established third-party data sharing/storage policies with most or all Third-Party vendors ● Incident Response Plan has been created and shared with responsible parties ● Policies and procedures are scheduled for ongoing review and a plan is in place to communicate policy changes to students, faculty, and parents via multiple communication channels: district Website, email, social media, and or communication systems

Submission Context:

Denville School District utilizes many tools to ensure the safety and security of onsite and hosted data. The district has policies to ensure the physical security of technology equipment. Building doors are secured with proximity access controls with printed, coded badges using Vanderbuilt Bright Blue System. This system allows different times and different building access per card. This system tracks entrance and exit using the proximity access for review as needed. The system also produces alerts if doors are left open. All technology closets in all buildings are secured with a lock and key. There are also security cameras recording in many locations throughout the buildings. Visitors must buzz to be let into a vestibule where they use our Lobby Guard Security System where they must scan their drivers license to gain access to our buildings. Once they are cleared and have a valid reason to enter the building, they report to the main office. The Board Office and Child Study Team Offices also have doors locked at all times with a 2n video door buzzer to allow in guests.

For data security back-up procedures are set for system files, libraries, and data. Disaster recovery plans are up to date and password protection and resources security is in place.

Cisco Advanced Malware Protection (AMP) is deployed to protect all devices and servers on the network. Cisco Firepower is used for firewall protection of the network. The schools and transportation garage use a Cisco 5545ASA firewall. The Board of Education offices use a Cisco 5516ASA firewall. Teachers, administrators and students have unique account credentials for logging onto the network via Microsoft Active Directory Group Policy. The district utilizes Google for Education for its email and applications, with all data stored in the cloud. Google for Education has industry leading safeguards and privacy policies. Data is secure, there are no ads on core services and it supports compliance with industry regulations and best practices. We have implemented Google 2 factor authentication for login to Google for Education as an option for all staff and require it for Technology Staff and Administrators.

The district also employs data security and privacy policies which both students and parents must sign at the beginning of the school year for data protection. An acceptable use of computer networks, computers and resources document which includes internet safety, Anti Big Brother and other policies must be signed in order to utilize computer services at the schools. These policies are available on our district website under Policies.

The technology team meets on a regular basis to discuss and security or privacy threats and outstanding work orders. The Technology Department receives emails from New Jersey Cybersecurity and Communications Integration Cell on current and new threats regularly. Staff is continually updated via the technology department for any security threats that it becomes aware of via emails or announcements. Professional Development classes for staff include data privacy and security issues. Homeland security holds classes for administrator and parents regarding security and privacy. Administrators teachers and parents recently attended a homeland security class to learn the latest security. We are testing Cofense, GoPhishMe to assist with training staff what to look for as tips for security risks in email.

Data security policies are also in place for termination of employment, Supervisors must fill out an exit form to initiate the process of deactivating a user from our systems. Upon an employee or administrator's termination, all accounts are immediately locked for Active Directory, Google, Frontline Applications, Student Information Systems. Badges are deactivated. Voicemail passwords are reset and the voicemail extension is either reassigned or marked as available for incoming staff.

***Evide*nce Links:**

Use this section to provide links to individual evidence pieces. Do not exceed the maximum evidence piece count of 10 links for the Technology Theme.

Evidence Number	Hyperlinked Evidence Title
1.	District Policy - Use of Technology and Acceptable Use Of Computer Networks Policy
2.	Google Apps for Education Contract and Anti Big Brother Form
3.	District Systems and Software Lists
4.	Incident Response
5.	Systems 3000 Security Policy Email
6.	Genesis Privacy Policy
7.	Link to Frontline Commitment to Security
8.	SchoolMessenger Data Privacy and Security Primer
9.	Link to School Messenger online Privacy Statement
10.	Link to Google Privacy and Security Center